Обеспечение безопасности Вашей организации в Интернете

Почему кибербезопасность важна для общественных групп и организаций?

На этой странице Вы найдете советы и некоторые шаги, которые Вы можете предпринять, чтобы защитить свою общественную группу или организацию от угроз кибербезопасности. Также существует отдельное руководство для физических лиц по обеспечению их собственной безопасности в Интернете.

Эти советы основаны на наиболее распространённых и серьёзных угрозах.

- Обновления - регулярно обновляйте программное обеспечение на своих устройствах, чтобы устранить любые уязвимые места в системе безопасности.
    - Регулярно обновляйте устройства своей общественной группы или организации. К ним относятся телефоны, компьютеры, WiFi-роутеры и все остальные устройства, которые подключаются к Интернету, включая смарт-устройства.
    - По возможности используйте автоматические обновления.
- Двухфакторная (двухуровневая) аутентификация (2FA) - повышает безопасность Ваших учётных записей, так как требует ввода пароля и выполнения дополнительного шага, например, ввода кода из приложения на Вашем телефоне.
    - Примечание: Эта технология также известна как многофакторная аутентификация (MFA), двухэтапная проверка (2SV) и под другими названиями.
    - Включите 2FA для всех учётных записей (аккаунтов) Вашей общественной группы или организации.
    - По возможности используйте формы 2FA, устойчивые к фишинговым атакам. Это защитит Вас от попыток обманом выманить данные. Примеры таких методов - физический ключ безопасности, отпечаток пальца или распознавание лица.
- Следите за безопасностью Ваших аккаунтов в Интернете - убедитесь, что бывшие участники не сохраняют доступ к аккаунтам после выхода из общественной группы или организации.
    - Если доступ к одному и тому же аккаунту имеет несколько человек, убедитесь, что у каждого есть отдельный логин и включена 2FA.
    - Ведите список всех аккаунтов пользователей и своевременно деактивируйте те, которые больше не используются, например, когда сотрудники покидают организацию.
    - Ведите учёт всех устройств, которые Вы выдавали членам своей организации, и не забывайте забирать их обратно и сбрасывать до заводских настроек, если сотрудники покидают организацию. Вам также может потребоваться изменить физические коды для доступа в здание.
- Проверьте, у кого есть доступ к Вашим аккаунтам в Интернете - люди в Вашей общественной группе или организации должны иметь доступ только к тому, что им нужно.

- Если аккаунт одного человека будет взломан, эти шаги ограничат вред, который может нанести злоумышленник.
- Регулярно проверяйте и удаляйте ненужные разрешения.
- Если у Вас есть один аккаунт администратора, который используют несколько человек, отслеживайте его на предмет необычной активности. Постарайтесь ограничить использование подобных аккаунтов, особенно для повседневных задач.
- Эти правила также применяются к доступу администратора к устройствам, таким как роутеры.

- Пересмотрите свои контракты с поставщиками услуг - если Вы наняли кого-либо для предоставления Вам ИТ-услуг.
    - Убедитесь, что у них есть средства кибербезопасности, соответствующие потребностям Вашей общественной группы или организации.
- Изучите взаимодействие Ваших аккаунтов и систем - понимание связей между ними поможет выявить уязвимые места, которые злоумышленники могут использовать.
    - Проверьте, как связаны Ваши системы, такие как электронная почта, облачное хранилище и бухгалтерские платформы.
    - Рассмотрите возможность использования виртуальной частной сети (VPN) для дополнительной безопасности в Интернете. Использование VPN скрывает Вашу онлайн-активность от тех, кто может попытаться Вас отслеживать. Это особенно полезно, если какие-либо члены Вашей общественной группы или организации подключаются удалённо.
- Поддерживайте «кибер-знания» своих сотрудников: люди в Вашей общественной группе или организации с большей вероятностью чаще становятся мишенью, чем системы.
    - Обучите всех сотрудников основам кибербезопасности. Сайт Own Your Online Own Your Online | NCSC предлагает широкий спектр советов и рекомендаций, которые помогут Вам обеспечить свою безопасность в Интернете и распознать мошенничество.
    - Напомните им, что это важно как для их личных аккаунтов, так и для аккаунтов, которые они используют в Вашей организации.
    - У нас также есть руководство для физических лиц по обеспечению их собственной безопасности в Интернете.
- Составьте план действий на случай инцидента - важно иметь план реагирования, чтобы люди не поддавались панике в случае инцидента.
    - План реагирования на инциденты описывает, кто что делает во время инцидента. Шаблоны доступны здесь Управление инцидентами | NCSC
    - Включите в свой план специальные действия на случай сбоя телефонов, компьютеров или других систем. Регулярно обновляйте этот план.

- Имейте под рукой контактные данные всех необходимых лиц, а также резервные способы связи, если основной способ связи, например, электронная почта, станет недоступным.
- Сохраните план где-нибудь вне своей системы, чтобы иметь к нему доступ в случае блокировки.